PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-113048
(43)Date of publication of application : 21.04.2000

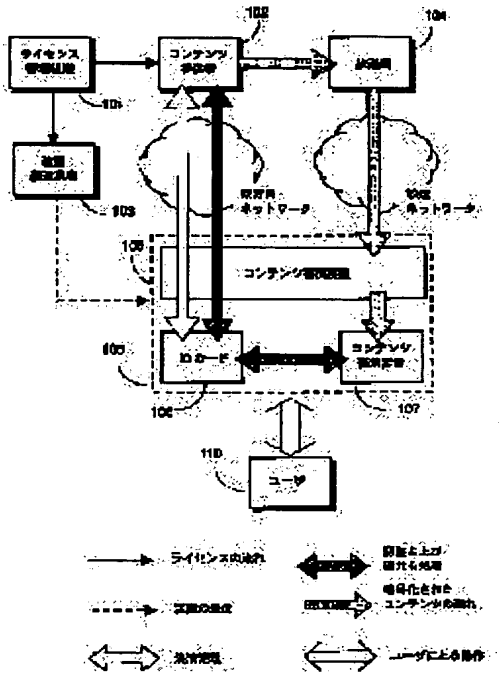
(51)Int.Cl. G06F 17/60
G09C 1/00
H04L 9/32
H04N 7/167
H04N 7/173

(21)Application number : 10-279597
(22)Date of filing : 01.10.1998

(71)Applicant : HITACHI LTD
(72)Inventor : AIKAWA SHIN
KUWABARA TEIJI

(54) CONTENTS RECEIVER GROUP AND IC CARD TO BE USED FOR THE SAME

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a contents receiver group having a function for protecting the copyright of digital contents from being violated by an illegal copy or falsification in the case of distributing the digital contents through a network.
SOLUTION: The contents receiver group 105 is constituted of an IC card 106 to be used for purchasing contents and protecting the copyright, a contents storage device 108 to be used for receiving and storing the purchased contents and a contents display device 107 to be used for displaying the purchased contents. Then, the IC card 106 and contents display device 107 have license information issued by a license managing organization.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号
特開2000－113048
（P2000－113048A）
(43)公開日　平成12年４月21日(2000.4.21)

(51)Int.Cl.[7]	識別記号	ＦＩ		テーマコード（参考）
Ｇ０６Ｆ　17/60		Ｇ０６Ｆ　15/21	３３０	５Ｂ０４９
Ｇ０９Ｃ　1/00	６６０	Ｇ０９Ｃ　1/00	６６０Ａ	５Ｃ０６４
			６６０Ｅ	５Ｊ１０４
Ｈ０４Ｌ　9/32		Ｈ０４Ｎ　7/173	６４０Ｚ	
Ｈ０４Ｎ　7/167		Ｇ０６Ｆ　15/21	Ｚ	

審査請求　未請求　請求項の数９　ＯＬ　（全 16 頁）　最終頁に続く

(21)出願番号　特願平10－279597

(22)出願日　平成10年10月１日(1998.10.1)

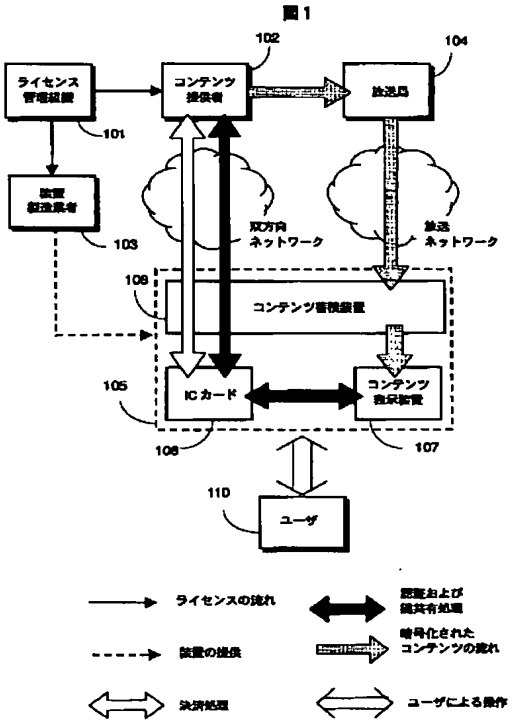
(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地
(72)発明者　相川　慎
神奈川県横浜市戸塚区吉田町292番地株式会社日立製作所マルチメディアシステム開発本部内
(72)発明者　桑原　禎司
神奈川県横浜市戸塚区吉田町292番地株式会社日立製作所マルチメディアシステム開発本部内
(74)代理人　100068504
弁理士　小川　勝男

最終頁に続く

(54)【発明の名称】　コンテンツ受信装置群およびそれに用いるＩＣカード

(57)【要約】
【課題】デジタルコンテンツをネットワークを介して流通させる際に、デジタルコンテンツの著作権を不正コピーや改ざんなどによって侵害されないように保護する機能を有する、コンテンツ受信装置群を提供することにある。
【解決手段】本発明におけるコンテンツ受信装置群は、コンテンツの購入および著作権保護に用いるICカードと、購入したコンテンツの受信及び蓄積に用いるコンテンツ蓄積装置と、購入したコンテンツの表示に用いるコンテンツ表示装置とから構成され、ICカードとコンテンツ表示装置は、ライセンス管理組織が発行した、ライセンス情報を有する。

図1



1

【特許請求の範囲】

【請求項１】コンテンツの購入、受信、蓄積、表示、著作権保護を行う装置群であって、

コンテンツの購入および著作権保護に用いるICカードと、

購入したコンテンツの受信及び蓄積に用いるコンテンツ蓄積装置と、

購入したコンテンツの表示に用いるコンテンツ表示装置と、から構成されるコンテンツ受信装置群において、

前記ICカードは、コンテンツ提供者から公開鍵暗号方式を用いてユーザ鍵を取得し、

前記コンテンツ蓄積装置は、共通鍵暗号方式で暗号化したコンテンツおよび共通鍵暗号方式で暗号化したコンテンツ鍵を受信して蓄積し、

前記コンテンツ蓄積装置は、前記蓄積装置から前記共通鍵暗号方式で暗号化したコンテンツおよび前記共通鍵暗号方式で暗号化したコンテンツ鍵を取得後、前記共通鍵暗号方式で暗号化したコンテンツ鍵を前記ICカードに渡し、

前記ICカードは、前記共通鍵暗号方式で暗号化したコンテンツ鍵を、前記ユーザ鍵で復号化した後、前記コンテンツ表示装置の公開鍵を用いた公開鍵暗号方式で暗号化して、前記コンテンツ表示装置に渡し、

前記コンテンツ表示装置は、前記公開鍵暗号方式で暗号化したコンテンツ鍵を、前記コンテンツ表示装置の秘密鍵で復号化した後、前記復号したコンテンツ鍵で、前記共通鍵暗号方式で暗号化したコンテンツを復号することを特徴とするコンテンツ受信装置群。

【請求項２】前記ICカードは、コンテンツの著作権を保護するためのメカニズムを提供するライセンス管理組織が発行したライセンス情報Aと、

前記ライセンス情報AとICカードを制御するための制御情報Aを保持するための情報保持部Aとを有し、

前記ライセンス情報Aは、デジタル証明書Aと、認証秘密鍵Aと、センタ公開鍵で構成され、

前記デジタル証明書Aは、ライセンス識別情報Aと、前記認証秘密鍵Aと対である認証公開鍵Aと、デジタル署名Aからなるものであり、

前記デジタル署名Aは、前記センタ公開鍵と対であって前記ライセンス管理組織が保持するセンタ秘密鍵を用いて作成された、前記認証公開鍵Aおよびライセンス識別情報Aに対するデジタル署名であり、

コンテンツ提供者からコンテンツの購入手続きを行う場合に、前記ライセンス情報Aを用いて、デジタル署名による相手認証を行い、前記デジタル署名による相手認証が成功すると、前記コンテンツ提供者から、ユーザ鍵と、コンテンツの識別情報を、前記ライセンス情報Aを用いて取得し、これらを前記制御情報Aとして、前記情報保持部Aに保存することを特徴とする請求項１記載のコンテンツ受信装置群。

2

【請求項３】前記コンテンツ蓄積装置は、コンテンツ蓄積装置を制御するための制御情報Cを保持する情報保持部Cと、コンテンツを蓄積するコンテンツ蓄積部Cを有し、

前記ICカードから、前記ICカードが保持している前記ライセンス情報A内のライセンス識別情報Aと、前記ICカードを用いて購入したコンテンツの識別情報とを、前記制御情報Cとして、前記情報保持部Cに保存し、

前記コンテンツ提供者あるいは前記コンテンツ提供者が依頼した放送局から、前記共通鍵暗号方式で暗号化したコンテンツと、前記共通鍵暗号方式で暗号化したコンテンツ鍵と、前記コンテンツの識別情報と、前記ライセンス識別情報Aとを受信し、

前記制御情報Cに、前記コンテンツ識別情報が存在していれば、前記共通鍵暗号方式で暗号化したコンテンツを、前記コンテンツ蓄積部Cに蓄積し、

前記制御情報Cに、前記ライセンス識別情報Aが存在していれば、前記共通鍵暗号方式で暗号化したコンテンツ鍵を、前記コンテンツ蓄積部Cに蓄積する、データ選択機能を有することを特徴とする、請求項１記載のコンテンツ受信装置群。

【請求項４】前記コンテンツ表示装置は、コンテンツの著作権を保護するためのメカニズムを提供するライセンス管理組織が発行したライセンス情報Bと、前記ライセンス情報Bを保持するための情報保持部Bと、コンテンツを蓄積するコンテンツ蓄積部Bと、コンテンツを表示するコンテンツ表示部とを有し、

前記ライセンス情報Bは、デジタル証明書Bと、認証秘密鍵Bと、センタ公開鍵で構成され、

前記デジタル証明書Bは、ライセンス識別情報Bと、前記認証秘密鍵Bと対である認証公開鍵Bと、デジタル署名Bからなるものであり、

前記デジタル署名Bは、前記センタ公開鍵と対であって前記ライセンス管理組織が保持しているセンタ秘密鍵を用いて作成された、前記認証公開鍵Bおよびライセンス識別情報Bに対するデジタル署名であり、

前記コンテンツ蓄積装置から、前記コンテンツ蓄積部Cに蓄積されている、前記共通鍵暗号方式で暗号化したコンテンツと、前記共通鍵暗号方式で暗号化したコンテンツ鍵と、前記コンテンツ識別情報と、前記ライセンス識別情報Aと、を受信し前記コンテンツ蓄積部Bに保存することを特徴とする請求項１記載のコンテンツ受信装置群。

【請求項５】前記コンテンツ表示装置は、前記ICカードに、コンテンツ鍵復号処理を要求するものであり、

前記コンテンツ鍵復号処理において、はじめに、前記コンテンツ表示装置は前記ライセンス情報Bを用い、前記ICカードは前記ライセンス情報Ａを用いてデジタル署名による相手認証を行い、

前記デジタル署名による相手認証が成功した後、前記IC

カードに、前記共通鍵暗号方式で暗号化したコンテンツ鍵を送信することを特徴とする、請求項１記載のコンテンツ受信装置群。

【請求項６】前記ICカードは、前記共通鍵暗号方式で暗号化したコンテンツ鍵を、前記ユーザを用いて復号化した後、前記認証公開鍵Bを用いた公開鍵暗号方式で暗号化して、前記コンテンツ表示装置に送信することを特徴とする、請求項１記載のコンテンツ受信装置群。

【請求項７】コンテンツ表示装置は、前記公開鍵暗号方式で暗号化したコンテンツ鍵を、前記認証秘密鍵Ｂを用いて復号化後、前記復号化したコンテンツ鍵を用いて、前記共通鍵暗号方式で暗号化したコンテンツを復号化し、前記復号化したコンテンツを、前記表示部に表示することを特徴とする、請求項１記載のコンテンツ受信装置群。

【請求項８】コンテンツの購入および著作権保護に用いるICカードにおいて、

コンテンツの著作権を保護するためのメカニズムを提供するライセンス管理組織が発行したライセンス情報と、前記ライセンス情報とICカードを制御するための制御情報を保持するための情報保持部とを有し、

前記ライセンス情報は、デジタル証明書と、認証秘密鍵と、センタ公開鍵で構成され、前記デジタル証明書は、ライセンス識別情報と、前記認証秘密鍵と対である認証公開鍵と、デジタル署名からなるものであり、

前記デジタル署名は、前記センタ公開鍵と対であって前記ライセンス管理組織が保持するセンタ秘密鍵を用いて作成された、前記認証公開鍵およびライセンス識別情報に対するデジタル署名であり、

コンテンツ提供者からコンテンツの購入手続きを行う場合に、前記ライセンス情報Aを用いて、デジタル署名による相手認証を行い、前記デジタル署名による相手認証が成功すると、前記コンテンツ提供者から、コンテンツを復号するための情報と、コンテンツの識別情報を、前記ライセンス情報を用いて取得し、これらを前記制御情報として、前記情報保持部に保存することを特徴とするICカード。

【請求項９】前記ICカードは、前記コンテンツ提供者が作成した共通鍵暗号方式で暗号化したコンテンツ鍵を取得すると、前記ユーザを用いて復号化した後、公開鍵暗号方式で暗号化して、外部に出力することを特徴とする請求項８記載のICカード。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、ネットワークを通じて映像や音楽等のディジタルコンテンツを流通させるためのシステム及びコンテンツ受信装置に関するものである。

【０００２】

【従来の技術】近年、コンピュータ技術の発展、インターネットの普及などにより、オンラインで、商品の購入手続きをする機会が増えてきた。また、従来はアナログ情報であった映像や音楽データが、CDやDVDなどのデジタルメディアで流通するようになった。今後は、映像や音楽などのデジタルデータを、インターネットなどのネットワーク上で購入し、デジタル蓄積装置にその場でダウンロードする形態が普及していくであろう。たとえば、現在、MP3フォーマットの音楽データが、インターネット上で急速に普及している。MP3は、MPEG1オーディオのレイヤIIIと呼ばれるデータ圧縮方式の通称である。M3フォーマットの音楽データは容易に、インターネットからダウンロードでき、例えば、パソコンで受信、蓄積および再生ができる。最近ではMP3データを再生できるプレーヤも登場している。

【０００３】

【発明が解決しようとしている課題】しかし、デジタルデータは、複製や変造が容易であり、ネットワークを介して複製を容易に転送できてしまう。したがって、著作権のある映画や音楽などのデジタルコンテンツをそのまま、ネットワーク上に流通させてしまうと、不正コピーなどにより、著作権を侵害される恐れがある。

【０００４】本発明の目的は、デジタルコンテンツをネットワークを介して流通させる際に、デジタルコンテンツの著作権を不正コピーや改ざんなどによって侵害されないように保護する機能を有する、コンテンツ受信装置群を提供することにある。

【０００５】

【課題を解決するための手段】上記目的を達成するために、本発明におけるコンテンツ受信装置群は、コンテンツの購入および著作権保護に用いるICカードと、購入したコンテンツの受信及び蓄積に用いるコンテンツ蓄積装置と、購入したコンテンツの表示に用いるコンテンツ表示装置とから構成され、ICカードとコンテンツ表示装置は、ライセンス管理組織が発行した、ライセンス情報を保持する。同様に本発明におけるコンテンツ提供者も、ライセンス管理組織が発行した、ライセンス情報を保持する。そして、このライセンス情報を用いて、相手認証および暗号通信を行うことで、コンテンツの不正コピーや改ざんが起こらないように、コンテンツを安全にネットワーク上に流通させることで、本発明におけるコンテンツ受信装置群で、受信、蓄積および視聴を行うことが出来る。

【０００６】

【発明の実施の形態】以下、本発明の実施の形態を図面を用いて説明する。図１は、本発明における電子流通システム全体のブロック図を表す。この電子流通システムは、ライセンス管理組織101、コンテンツ提供者102、装置製造業者103、放送局104、コンテンツ受信装置群105およびユーザ110から成る。コンテンツ受信装置群105は、ICカード106、コンテンツ表示装置107およびコンテ

ンツ蓄積装置108から成る。

【０００７】ライセンス管理組織101は、コンテンツの著作権を保護するためのメカニズムをコンテンツ提供者102および装置製造業者103に提供する。装置製造業者103は、ライセンス管理組織101から取得したライセンス情報をもとに、コンテンツ受信装置群105を製造する。以下、この電子流通システムを用いた、コンテンツの著作権保護の仕組について説明する。

【０００８】ユーザ110は、コンテンツ受信装置群105を購入し、これらを用いてコンテンツの購入、受信、蓄積および視聴を行う。ユーザ110は、まず、ICカード106をコンテンツ蓄積装置108に接続し、コンテンツ提供者102との間で、双方向ネットワークを介して、コンテンツの購入を行う。ここで、双方向ネットワークは、任意のものでよく、例えば、インターネットや電話網が考えられる。コンテンツの購入は、決済処理と著作権保護のための認証処理から成る。決済処理は任意のものを用いてよい。一方で、著作権保護のための認証処理としては、ライセンス管理組織101が発行したライセンス情報を用いて、コンテンツ提供者102とICカード106の両者で相手認証を行う。この認証が成功すると、続いて、ICカード106は、コンテンツを復号化するための情報と、購入したコンテンツの識別情報をコンテンツ提供者102から安全に取得し、内部に保存する。ここで、情報を安全に取得するという意味は、送受信する情報が、第三者に盗聴されたり、改ざんされたりすることが起こらないことをいい、以下同様に用いる。また、ICカード106は、外部から内部の情報を不正に取得できないように出来ており、以下このような装置をタンパーレジスタントモジュールと呼ぶ。またコンテンツ表示装置107もICカードと同様にタンパーレジスタントモジュールで構成されている。

【０００９】次に、コンテンツ提供者102は、コンテンツを暗号化し、暗号化したコンテンツと、それに対応する暗号化したコンテンツ鍵、コンテンツの識別情報、およびコンテンツを購入したユーザが所有するICカードの識別情報を、配信してもらうよう放送局104に依頼する。ここで、コンテンツ鍵は、コンテンツを暗号化するために用いた鍵である。また、コンテンツの暗号化およびコンテンツ鍵の暗号化はそれぞれ、共通鍵暗号方式であれば任意のものであってよい。放送局104は、放送ネットワークを介して、ユーザ110にそれらの情報を配信する。ここで、放送ネットワークは任意のものでよく、例えば、地上波放送、衛星放送、ケーブル放送あるいは、インターネットが考えられる。また、放送局104はコンテンツ提供者102自身でもよい。暗号化したコンテンツは、それに対応する暗号化したコンテンツ鍵およびコンテンツの識別情報と共に、ユーザ110が所有するコンテンツ蓄積装置108によって、受信、蓄積される。ここで、コンテンツ蓄積装置108は、購入したコンテンツの識別情報、および購入時に用いたICカードの識別情報が保存されていて、該当するコンテンツのみを蓄積する、フィルタリング機能を有する。

【００１０】ユーザ110がコンテンツを視聴したいと思った場合は、まず、コンテンツ蓄積装置108に蓄積されている、ユーザが視聴したいと思う、暗号化したコンテンツと、それに対応する、暗号化したコンテンツ鍵、コンテンツの識別情報、およびそのコンテンツを購入したときに用いたICカードの識別情報を、コンテンツ表示装置107に転送する。次に、ICカード106をコンテンツ表示装置107に接続し、ICカード106とコンテンツ表示装置107との間で、ライセンス管理機関101が発行したライセンス情報を用いて、著作権保護のための相手認証処理を行う。この認証処理が成功すると、コンテンツ表示装置107は、接続されたICカード106の識別情報が、表示させたいコンテンツを購入したときに用いたICカードの識別情報と一致するかを検査する。もし一致すれば、続いてコンテンツ表示装置107は、暗号化したコンテンツ鍵とコンテンツの識別情報をICカード106に転送する。ICカード106は、コンテンツ表示装置107から取得したコンテンツの識別情報に対応した、コンテンツを復号化するための情報を用いて、暗号化したコンテンツ鍵を復号化し、再び、コンテンツ表示装置107にしか解読できないように暗号化して、コンテンツ表示装置107に渡す（詳細は後述する）。そして、コンテンツ表示装置107は、ICカード102から受け取ったコンテンツ鍵を復号化して、それを用いてコンテンツを復号化し、コンテンツを表示させる。

【００１１】以上の方法によって、コンテンツを購入したユーザしか、そのコンテンツを視聴することが出来きない。また、外部の通信路を流れるコンテンツや秘密情報はすべて暗号化されているため、第三者による、コンテンツの不正コピーや改ざんを防止し、コンテンツの著作権を保護することが可能になる。図１において、コンテンツ蓄積装置108は、コンピュータであってもよい。また、セットトップボックスなどの専用装置であってもよい。また、ICカードは、非接触型で、コンテンツ蓄積装置108やコンテンツ表示装置107に挿入しなくてもよいものであってもよい。

【００１２】次に、ライセンス管理組織101が発行するライセンス情報について説明する。図２は、ライセンス管理組織101がコンテンツ提供者102および装置製造業者103に渡すライセンス情報を表している。コンテンツ提供者102は、ライセンス管理組織101からライセンス情報201を安全に取得する。ライセンス情報201は、デジタル証明書202、認証秘密鍵203およびセンタ公開鍵210から成る。デジタル証明書202は、ライセンスID 205、認証公開鍵206およびデジタル署名207から成る。認証秘密鍵203および認証公開鍵206は、公開鍵暗号方式における秘密鍵および公開鍵の対であり、各ライセンス情報毎に異なる値である。ライセンスID 205は、ライセンス情報の

識別情報であり、ライセンス情報毎に異なる値である。センタ公開鍵210は、公開鍵暗号方式における公開鍵であり、ライセンス管理組織101が管理しているセンタ秘密鍵211と対をなすものである。デジタル署名207は、ライセンス管理組織101が、ライセンスID 205と認証公開鍵207から、センタ秘密鍵211を用いて生成したデジタル署名である。デジタル署名207は、センタ公開鍵210を用いて検証することができる。デジタル署名207の検証が成功すれば、認証公開鍵206およびライセンスID205が正しいことを証明できる。上述した情報の内、センタ秘密鍵211と認証秘密鍵203は秘密情報であり、外部に漏洩しないように管理する必要がある。

【００１３】同様に、装置製造業者は、ライセンス管理組織101から、Ｌ個のライセンス情報2211～201Lを安全に取得する。ライセンス情報2211～201Lの構成は、先に述べたライセンス情報201の構成と同様である。ここで、本発明で用いる公開鍵暗号方式は任意のものでよい。たとえば、楕円曲線暗号などが挙げられる。同様に、本発明で用いるデジタル署名の生成方法も任意の方法を用いてよい。たとえば、DSA署名が挙げられる。これらについては、岡本龍明著「現代暗号」（産業図書）に詳しい。

【００１４】次に、装置製造業者103がコンテンツ受信装置群105を製造する場合について説明する。図３は、装置製造業者103によるコンテンツ受信装置群105の製造方法を示している。図３において、装置製造業者103は、コンテンツ受信装置群105を製造する際に、ライセンス管理組織101から取得したライセンス情報2211～201Lのうち、任意のライセンス情報221iをICカード106の内部に埋め込む。同様に任意のライセンス情報221jをコンテンツ表示装置107に埋め込む。本発明においては、コンテンツ受信装置108には、ライセンス情報は埋め込まないものとする。

【００１５】次に、コンテンツ受信装置群105の構成について説明する。図４は、コンテンツ受信装置群105の詳細ブロック図である。ICカード106は、ICカードインタフェイス400、情報処理部401、情報保持部402、プログラム保持部403から成り、それぞれが内部バスで接続されている。コンテンツ表示装置107は、コンテンツ転送インタフェイス410、ICカードインタフェイス411、情報処理部412、情報保持部413、コンテンツ蓄積部414、プログラム保持部415、表示部416、ユーザ入力部417から成り、それぞれが内部バスで接続されている。コンテンツ蓄積装置108は、放送受信部420、ネットワークインタフェイス421、コンテンツ転送インタフェイス422、ICカードインタフェイス423、情報処理部424、情報保持部425、コンテンツ蓄積部426、プログラム保持部427、表示部428、ユーザ入力部429から成り、それぞれが内部バスで接続されている。

【００１６】次に、コンテンツ受信装置群105の情報処理について説明する。ICカードは、プログラム保持部403に保持されているプログラム、および情報保持部402に保持されている情報に従って、情報処理部401で情報処理を行う。また、情報処理部402の内容はICカードインタフェイス400を介して更新される。コンテンツ表示装置107は、プログラム保持部415に保持されているプログラム、および情報保持部413に保存されている情報に従って、情報処理部412で情報処理を行う。また、コンテンツ蓄積部414に蓄積されている、暗号化されているコンテンツを、情報処理部412で復号化し、表示部415に表示する。コンテンツ蓄積部414に蓄積されているコンテンツは、コンテンツ転送インタフェイス410を介して更新される。また、ユーザの操作をユーザ入力部416で感知し、情報処理部411で対応する処理を行い、結果を表示部415に表示する。

【００１７】コンテンツ蓄積装置108は、プログラム保持部427に保持されているプログラム、および情報保持部425に保存されている情報に従って、情報処理部424で情報処理を行う。また、ユーザの操作をユーザ入力部429で感知し、情報処理部424で対応する処理を行い、結果を表示部428に表示する。また、情報保持部425に保持されている情報は、ネットワークインタフェイス421およびICカードインタフェイス423を介して更新される。また、コンテンツ蓄積部426に蓄積されている情報は、放送受信部420を介して更新される。

【００１８】次に、コンテンツ受信装置群105の通信方法について説明する。ICカード106とコンテンツ表示装置107は、ICカードインタフェイス400および411を介して通信を行う。同様に、ICカード106とコンテンツ蓄積装置108は、ICカードインタフェイス400および423を介して通信を行う。コンテンツ表示装置107とコンテンツ蓄積装置108は、コンテンツ転送部410および422を介して、コンテンツを送受信する。また、コンテンツ蓄積装置108は、放送受信部420で放送データを受信し、ネットワークインタフェイス421で、双方向ネットワークに接続し、コンテンツ提供者102と通信を行う。

【００１９】以上、コンテンツ受信装置群105の構成について説明した。次に、コンテンツ受信装置群105に保存されている情報について詳細に説明する。図５は、ICカード106の情報保持部402に保持されている情報を表している。情報保持部402には、ライセンス管理組織101から取得した、デジタル証明書222i、認証秘密鍵223i、センタ公開鍵210、そして、コンテンツ提供者102から、著作権保護のための認証処理の結果取得した、K個の契約情報 5001～500Kが保存されている。それぞれの契約情報5001～500Kは、同様の構成であり、例えば、k番目の契約情報500kは、コンテンツID 501 kとユーザ鍵502kから成る。コンテンツID 501kは、購入したコンテンツの識別子である。また、ユーザ鍵502 kは、暗号化されたコンテンツを復号化するために用いる。詳細は後述す

る。

【００２０】次に、コンテンツ表示装置107の情報保持部413内部について詳細に説明する。図６は、情報保持部413に保持されている情報を表している。情報保持部413には、ライセンス管理組織101から取得した、デジタル証明書222j、認証秘密鍵223j、センタ公開鍵210が保持されている。

【００２１】次に、コンテンツ蓄積装置108の情報保持部425内部について詳細に説明する。図７は情報保持部425に保存されている情報を表している。情報保持部425には、S個の制御情報8001 ～800Sが保持されている。これらの情報は、コンテンツを購入する際に、コンテンツ提供者101から取得する。それぞれの制御情報8001 ～800Sは同様の構成であり、例えば、s番目の制御情報800sは、コンテンツID 801sおよびライセンスID 802sから成る。コンテンツID 801sは、制御情報800s をコンテンツ提供者から取得する際に購入したコンテンツの識別子であり、ライセンスID 802sは、その時使用したICカードのライセンス情報の識別子である。

【００２２】次に、コンテンツ表示装置107のコンテンツ蓄積部414内部について詳細に説明する。図８は、コンテンツ蓄積部414に蓄積されているコンテンツファイルを表している。コンテンツ蓄積部414には、M個のコンテンツファイル7001 ～700Mが蓄積されている。それぞれのコンテンツファイル7001 ～700Mは、同様の構成である。例えば、m番目のコンテンツファイル700mは、コンテンツID 701m、P個のライセンスID 702m1～702mP、P個の暗号化されたコンテンツ鍵703 m1～703 mP、そして、暗号化されたコンテンツデータ704mから成る。コンテンツID 701mはコンテンツファイル700m内のコンテンツの識別子である。それぞれのライセンスID702m1～702mPは、コンテンツファイル700 m内のコンテンツを、コンテンツ提供者102から購入する際に使用したICカードのライセンス情報の識別子である。また、それぞれの暗号化されたコンテンツ鍵703 m1～703 mPは、ＩＣカードがコンテンツ提供者から取得したユーザ鍵で暗号化されている。たとえば、コンテンツファイル700m内のp番目の暗号化されたコンテンツ鍵703 mpは、ライセンスID 702 mpを持つICカードの内部に保存されているユーザ鍵で暗号化されている。

【００２３】次に、コンテンツ蓄積装置108のコンテンツ蓄積部426内部について詳細に説明する。図９は、コンテンツ蓄積部426に保持されているコンテンツファイルを表している。コンテンツ蓄積部426には、N個のコンテンツファイル9001 ～900Nが蓄積されている。それぞれのコンテンツファイル9001 ～900Nは、図８を用いて説明した、コンテンツ7001 ～700Mと同様の構成である。

【００２４】以上、コンテンツ受信装置群105に保存されている情報について説明した。次に、コンテンツを放送局104が配信する時の、データフォーマットについて説明する。図１０は、本発明におけるコンテンツを配信するためのデータフォーマットである。図１０に示すように、コンテンツデータは、複数のパケット10001 ,...,1000i ,...に分割およびカプセル化されて配信される。それぞれのパケットは同様の構成であり、例えば、i番目のパケット1000iは、パケットヘッダ1001iと、ペイロード1002iで構成される。パケットヘッダ1001iにはパケットの制御情報が格納される。ペイロード1002iにはコンテンツが格納される。このようなパケットは任意のものを用いてよい。例えば、MPEG2-TSが考えられる。

【００２５】ペイロード1002 iは、図１０に示すように、選択番号1010 iとデータフレーム1011 iから成る。選択番号1010 iは、データフレーム1011 i内に格納されているデータを識別し、「0」か「1」の２値をとる。例えば、選択番号1010 iが「0」の場合、データフレーム1011 i内に格納されているデータは、図１０に示すように、コンテンツID 1020 i 、制御情報1021 i 、暗号化されたコンテンツフレーム1022 i から成る。暗号化されたコンテンツフレーム1022 i は、暗号化されたコンテンツデータそのもの、あるいはその一部であり、コンテンツ鍵によって暗号化されている。コンテンツID 1020 i は暗号化されたコンテンツフレーム1022i に対応するコンテンツの識別子である。また、制御情報1021 i は、暗号化されたコンテンツフレーム1022 iを暗号化されたコンテンツデータに組み立てるための制御情報である。

【００２６】一方で、選択番号1010 iが「1」の場合、データフレーム1011 i内に格納されているデータは、図１０に示すように、ライセンスID 1030 i 、制御情報1031 i、アクセス情報1032 i から成る。制御情報1031 i は、アクセス情報1032 i を処理するのに用いる。アクセス情報1032 i は、複数のコンテンツID 1040i 1,...,1040i j ,...、および、複数の暗号化されたコンテンツ鍵1050i 1,...,1050ij ,...から成る。ここで、コンテンツID1040 i jは、ライセンスID 1030 iを保持しているICカードを用いて、コンテンツ提供者から購入したコンテンツの識別子である。また、暗号化されたコンテンツ鍵は、ライセンスID 1030 iを保持しているICカードが取得したユーザ鍵で暗号化されている。

【００２７】以上、コンテンツを放送局104が配信する時の、データフォーマットについて説明した。次に、ICカード106をコンテンツ蓄積装置108に接続し、コンテンツ提供者102からコンテンツを購入する手続きについて詳細に説明する。図１１は、コンテンツを購入するための手続きのフローチャートである。まず、ICカード106をコンテンツ蓄積装置108に接続し、ICカード106とコンテンツ提供者102との間で、決済処理1100を行う。前述したように、決済処理1100は任意の方法を用いてよい。

決済処理1100が失敗したら、購入手続きは失敗する。決済処理1100が成功したら、続いて、著作権保護のための認証処理1101が行われる。著作権保護のための認証処理1101の詳細については後述する。著作権保護のための認証処理1101が失敗したら、購入手続きは失敗する。著作権保護のための認証処理1101が成功したら、つづいて、ユーザ鍵取得処理1102を行う。ユーザ鍵取得処理1102の詳細については後述する。ユーザ鍵取得処理1102が失敗したら、購入手続きは失敗する。ユーザ鍵取得処理1102が成功したら、購入したコンテンツのコンテンツIDと取得したユーザ鍵を契約情報として、ICカード内の情報保持部402に保存する（処理1103）。次に、購入したコンテンツのコンテンツIDと、使用したICカードのライセンスIDを制御情報として、コンテンツ蓄積装置108内の情報保持部425に保存する。以上のべたすべての処理が成功したら、コンテンツの購入手続きは成功する。

【００２８】次に、著作権保護のための認証処理1101の詳細を述べる。著作権保護のための認証処理1101は、ライセンス管理組織101が発行したライセンス情報を用いた相手認証であれば、どんな方法でもよい。例えば、図１２にその一例を示す。図１２は、コンテンツ提供者102とICカード106の相手認証のフロー図であり、デジタル署名を用いたチャレンジーレスポンス型の相手認証である。まず、ICカード106は、自分のデジタル証明書をコンテンツ提供者102に送信する（処理1200）。コンテンツ提供者102は、ICカード106から受け取ったデジタル証明書からデジタル署名を取り出し、それをセンタ公開鍵を用いて検証する(処理1201)。この検証によって、ICカード106から受信したデジタル証明書に含まれる、ICカード106の認証公開鍵が、ライセンス管理機関101が発行した正しいものであることが証明できる。この検証が失敗すれば、コンテンツ提供者102は、ICカード106を不正と見なし、認証を中断する。デジタル署名の検証が成功すると、続いて、コンテンツ提供者102は、ICカード106から受け取ったデジタル証明書から認証公開鍵を取りだし保存する(処理1202)。そして、チャレンジのための乱数を生成しICカード106に転送する(処理1203)。ICカードは、コンテンツ提供者102が生成したチャレンジ乱数に対するデジタル署名を、自分の認証秘密鍵を用いて生成し、レスポンスとして、コンテンツ提供者102に送信する(処理1204)。コンテンツ提供者102は、ICカード102から受信したレスポンスとしてのデジタル署名を、ICカード106の認証公開鍵を用いて検証する(処理1205)。この検証によって、ICカード106が、ライセンス管理組織101が発行した、正しい認証秘密鍵を保持していることを証明できる。この検証が失敗したら、コンテンツ提供者102は、ICカード106を不正と見なし、認証を中断する。成功すれば、コンテンツ提供者102は、ICカード106を認証する。以上の相手認証を、今度は、コンテンツ提供者102とICカード106が入れ替わって行えば、相互に相手を認証することができる。以上、著作権保護のための認証処理1101について説明した。

【００２９】次に、ユーザ鍵取得処理1102の詳細を述べる。ユーザ鍵取得処理1102は、ライセンス管理組織101が発行したライセンス情報をもとに、コンテンツ提供者が発行したユーザ鍵を、安全に、ICカードが取得できる方法であれば、どんな方法を用いてもよい。例えば、図１３にその一例を示す。図１３は、コンテンツ提供者102とICカード106の暗号通信のフロー図であり、公開鍵暗号方式を用いて、ユーザ鍵を安全に配送している。まず、コンテンツ提供者は、ユーザ鍵を生成する（処理1300）。そして先に取得した、ICカード106の認証公開鍵を用いてユーザ鍵を暗号化し、ICカード106に送信する（処理1301）。ICカード106は、コンテンツ提供者102から、暗号化されたユーザ鍵を受け取ると、自分の認証秘密鍵でそれを復号化する。以上の方法により、コンテンツ提供者102はICカード106にユーザ鍵を安全に送信できる。

【００３０】次に、コンテンツ蓄積装置108が、放送局104が配信するコンテンツを、取得する方法について説明する。図１４は、コンテンツ蓄積装置108がコンテンツを受信するフローチャートである。コンテンツ蓄積装置108は、コンテンツ蓄積装置108内の情報保持部425に格納されている制御情報に基づいて、コンテンツを受信し、受信したコンテンツを、コンテンツ蓄積装置108内のコンテンツ蓄積部426に蓄積していく。

【００３１】まず、コンテンツ蓄積装置108は、パケットを受信する（処理1400）。ここで、パケットフォーマットは、先に図１０を用いて説明したものと同じである。パケットを受信すると、パケット内から選択番号を検出する（処理1401）。選択番号に関しては、先に図１０を用いて説明した。もし選択番号が「0」であれば、このパケットには、暗号化されたコンテンツデータが格納されていると判断する。この場合、パケット内のコンテンツIDを検出し、これが、コンテンツ蓄積装置108内の情報保持部425に格納されいる、制御情報内のコンテンツIDに一致するかを走査していく(処理1404)。もし、一致すれば、このパケット内に格納されている、暗号化されたコンテンツデータを、コンテンツ蓄積装置108内のコンテンツ蓄積部426内に蓄積する（処理1406）。コンテンツをコンテンツ蓄積部426に蓄積する際の配置に関しては、先に図７を用いて説明した。一方で、もし選択番号が「1」であれば、このパケットには、アクセス情報が格納されていると判断する。この場合、パケット内のライセンスIDを検出し、これが、コンテンツ蓄積装置108内の情報保持部425に格納されいる、制御情報内のライセンスIDと一致するかを走査していく(処理1403)。もし、一致すれば、このパケット内に格納されている、アクセス情報を、コンテンツ蓄積装置108内のコンテンツ蓄積部426内に蓄積する（処理1406）。アクセス情報

をコンテンツ蓄積部426に蓄積する際の配置に関しては、先に図７を用いて説明した。

【００３２】以上の処理を、繰り返していくことで、コンテンツ蓄積装置108は、情報保持部425に格納されている制御情報に基づいて、コンテンツを受信し、受信したコンテンツを、コンテンツ蓄積部426に蓄積していく。これによって、必要なコンテンツだけを蓄積することができる。

【００３３】次に、コンテンツ蓄積装置108に格納されたコンテンツを、コンテンツ表示装置107を用いて、表示させる方法について述べる。図１５は、ICカード106とコンテンツ蓄積装置107の間で行う、コンテンツ表示手続きのフロー図である。ここで、予め、コンテンツ蓄積装置108から、コンテンツ表示装置107に、表示したいコンテンツを転送しておく。転送方法に関しては、先に図４を用いて説明した。まず、ICカード106をコンテンツ表示装置107に接続し、ICカード106とコンテンツ表示装置107との間で、著作権保護のための認証処理1500を行う。著作権保護のための認証処理1500は、先に図12を用いて説明した、ICカード106とコンテンツ提供者102との間の相手認証と同様である。著作権保護のための認証処理1500が失敗したら、コンテンツの表示手続きは失敗する。著作権保護のための認証処理1500が成功したら、つづいて、コンテンツ表示装置107は、先に行った、著作権保護のための認証処理1500で、ICカード106から受け取った、デジタル証明書内のライセンスIDが、コンテンツ表示装置107のコンテンツ蓄積部414に格納されている、表示させたいコンテンツファイル内のライセンスIDに一致するかを走査していく(処理1501)。もし、一致しなければ、コンテンツの表示手続きは失敗する。もし、一致すれば、コンテンツ表示装置107は、表示させたいコンテンツファイルのコンテンツIDと、そのコンテンツファイル内にあって、先に確認したＩＣカードのライセンスＩＤに対応する、暗号化されたコンテンツ鍵を、ICカード106に送信する(処理1502)。ICカード106は、コンテンツ表示装置107から、コンテンツIDおよび暗号化されたコンテンツ鍵を受け取ると、まず、受け取ったコンテンツIDが、ICカード106の情報保持部402に格納されている、契約情報内のコンテンツIDに一致するかを走査していく(処理1503)。もし、一致しなければ、コンテンツの表示手続きは失敗する。もし、一致すれば、ICカード106は、コンテンツ表示装置107から受け取った、暗号化されたコンテンツ鍵を、ICカード106の情報保持部402内にあって、処理1503で一致したコンテンツIDが格納されている、契約情報内のユーザ鍵を用いて、復号化する(処理1054)。続いて、ICカード106は、コンテンツ鍵を、先に著作権保護のための相手認証処理で取得した、コンテンツ蓄積装置107の認証公開鍵で暗号化し、コンテンツ表示装置107に返送する(処理1505)。コンテンツ表示装置107は、ICカード106から暗号化されたコンテンツ鍵を受け取ると、それを、自分の認証秘密鍵で復号化し、コンテンツ鍵を得る(処理1506)。続いて、取得したコンテンツ鍵で、表示させたいコンテンツファイル内の暗号化されたコンテンツデータを復号化し(処理1507)、コンテンツを表示させる(処理1508)。

【００３４】以上の手続きによって、コンテンツ蓄積装置107は、コンテンツ鍵を復号化し、それを用いてコンテンツを復号化して表示することが可能になる。また、コンテンツを購入した時に用いたICカードを、コンテンツ蓄積装置107に接続しなければ、コンテンツ蓄積装置107は、コンテンツ鍵を復号することが出来ず、コンテンツを表示できない。

【００３５】また、ICカード106とコンテンツ蓄積装置107の間の通信路上、さらに、ICカード106とコンテンツ提供者102の間の通信路上、コンテンツ提供者102とコンテンツ蓄積装置108の間の通信路上、およびコンテンツ蓄積装置108とコンテンツ表示装置107の間の通信路上を流れるコンテンツあるいは秘密情報は、すべて暗号化されているので、本発明による電子流通システムにおいては、流通するコンテンツが第三者により盗聴および改ざんされることはない。

【００３６】

【発明の効果】本発明により、デジタルコンテンツをネットワークを介して流通させる際に、デジタルコンテンツの著作権を不正コピーや改ざんなどによって侵害されないように保護する機能を有する、コンテンツ受信装置群を提供できる。

【図面の簡単な説明】

【図１】本発明の実施例に係る、電子流通システムの概要ブロック図。

【図２】ライセンス組織101がコンテンツ提供者102および装置製造業者103に渡すライセンス情報を表した図。

【図３】装置製造業者103によるコンテンツ受信装置群105の製造方法を表した図。

【図４】コンテンツ受信装置群105の詳細ブロック図。

【図５】ICカード106の情報保持部402に保持されている情報を表した図。

【図６】コンテンツ表示装置107の情報保持部413に保持されている情報を表した図。

【図７】コンテンツ蓄積装置108の情報保持部425に保存されている情報を表した図。

【図８】コンテンツ表示装置107のコンテンツ蓄積部に蓄積されているコンテンツファイルを表した図。

【図９】コンテンツ蓄積装置108のコンテンツ蓄積部426に保持されているコンテンツファイル情報を表した図。

【図１０】本発明の実施例に係るコンテンツを配信するためのデータフォーマットを表した図。

【図１１】本発明の実施例に係るコンテンツを購入するための手続きのフローチャート。

【図１２】コンテンツ提供者102とICカード106の相手認

証のフロー図。

【図１３】コンテンツ提供者102とICカード106の暗号通信のフロー図。

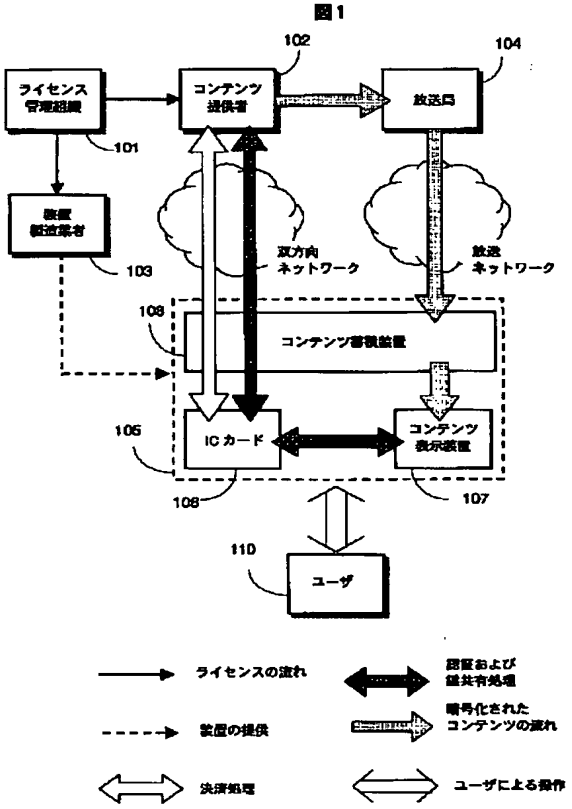
【図１４】コンテンツ蓄積装置108がコンテンツを受信するフローチャート。

【図１５】ICカード106とコンテンツ蓄積装置107の間で行う、コンテンツ表示手続きのフロー図。

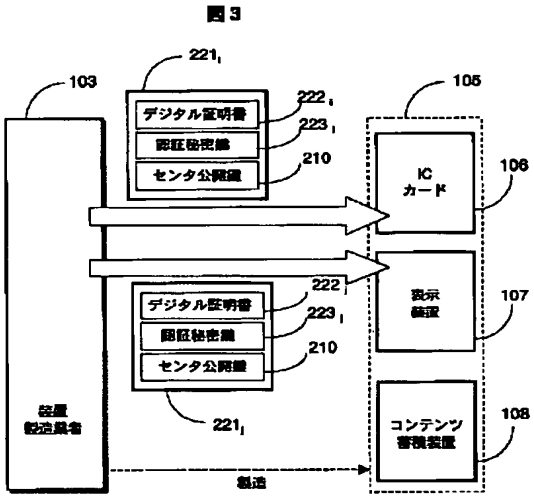
【符号の説明】

＊101・・・・ライセンス管理組織
102・・・・コンテンツ提供者
103・・・・装置製造業者
104・・・・放送局
105・・・・コンテンツ受信装置群
106・・・・ICカード
107・・・・コンテンツ表示装置
＊108・・・・コンテンツ蓄積装置

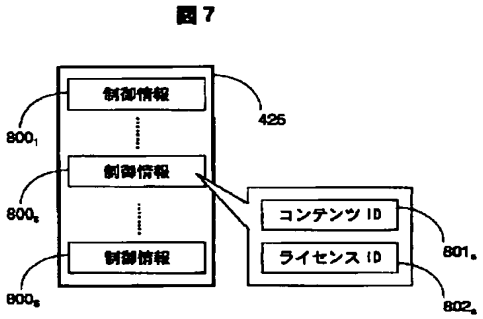
【図１】



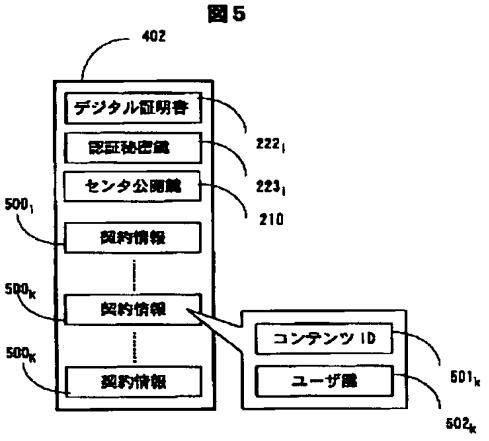
【図３】



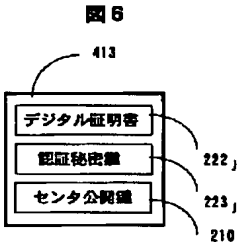
【図７】



【図５】

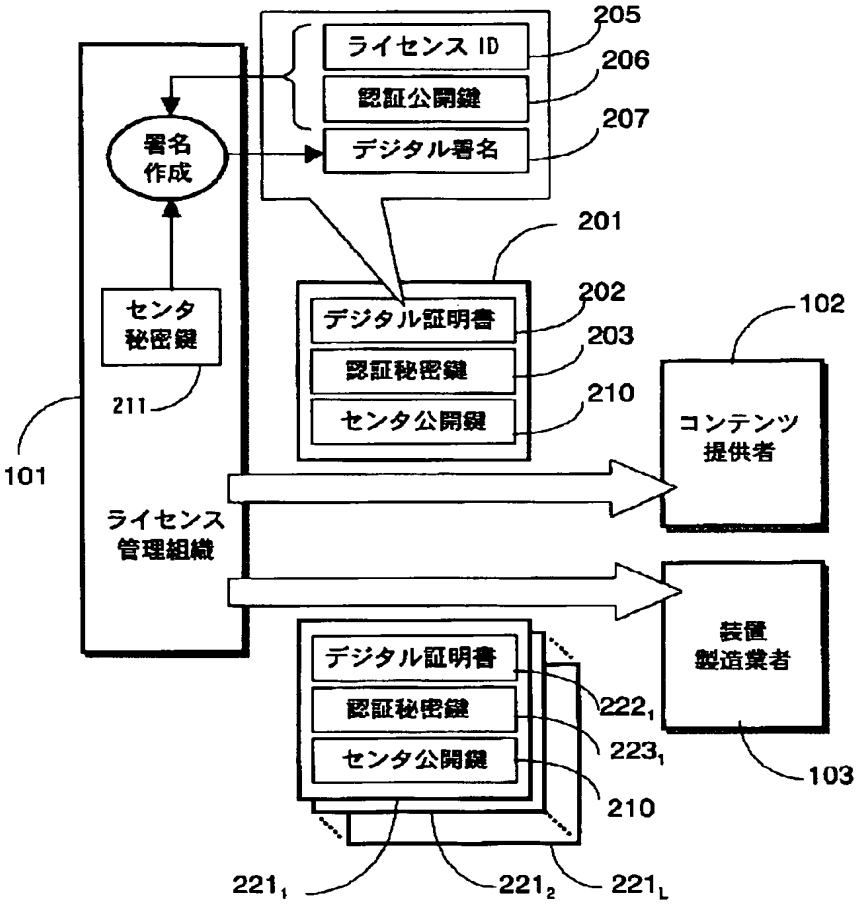


【図６】



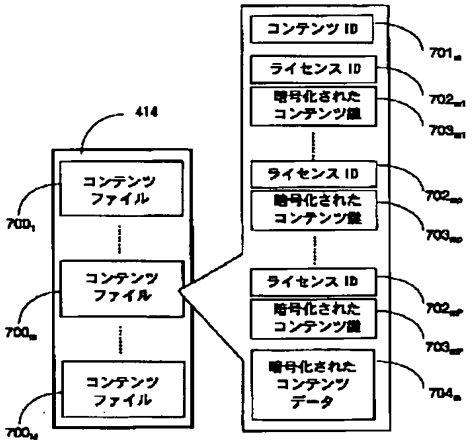
【図２】

図２



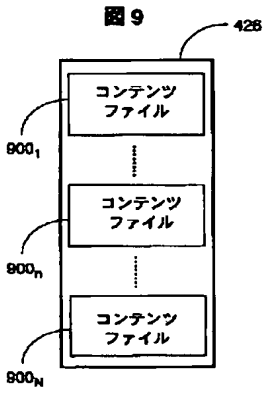
【図８】

図８



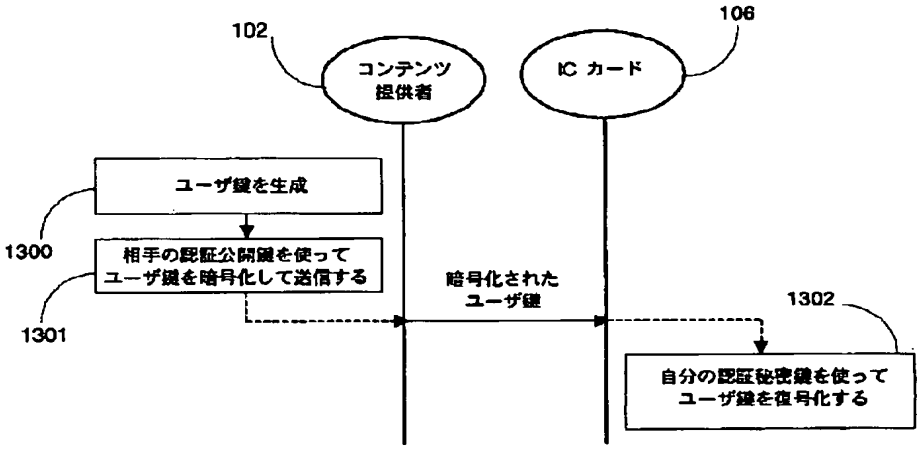
【図９】

図９



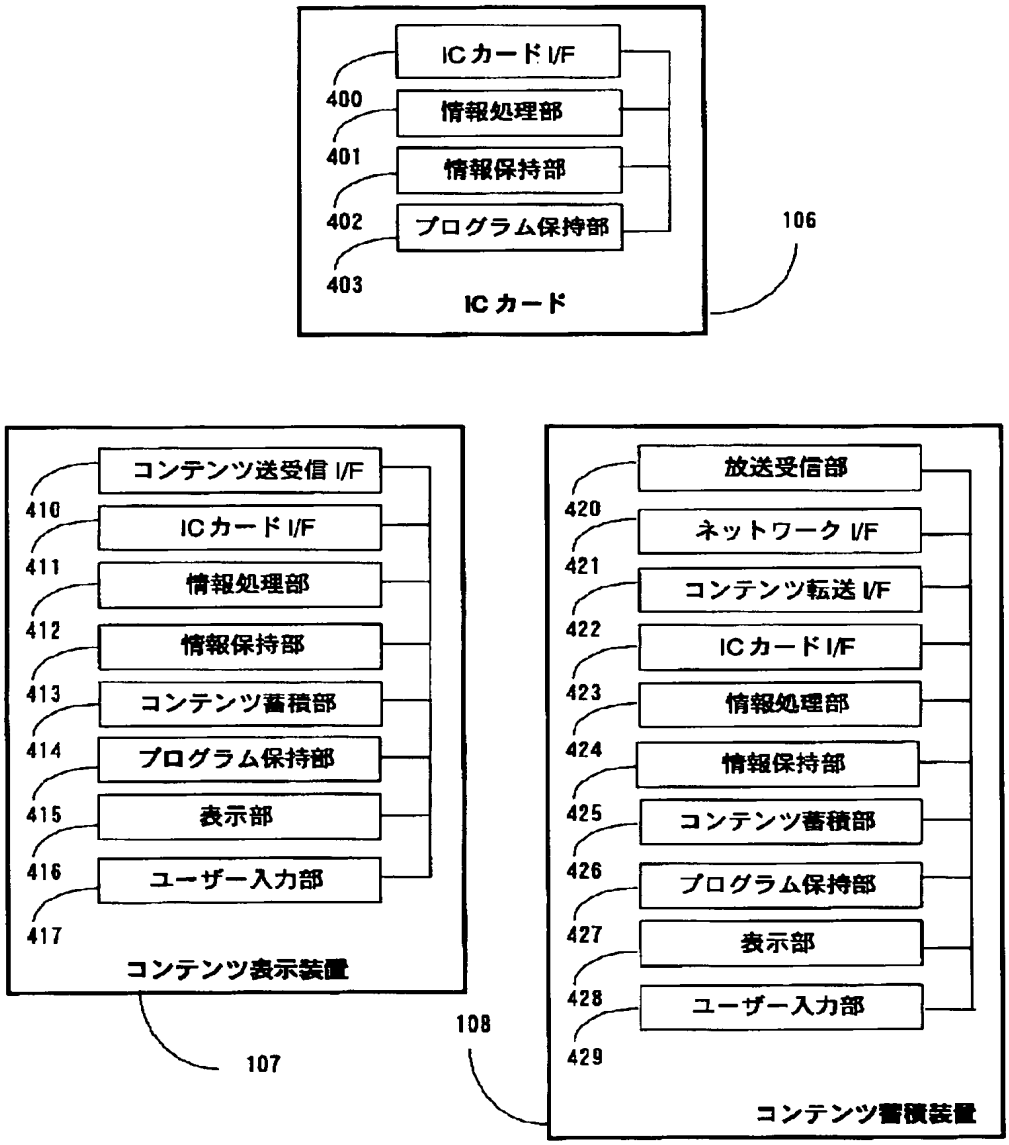
【図１３】

図１３



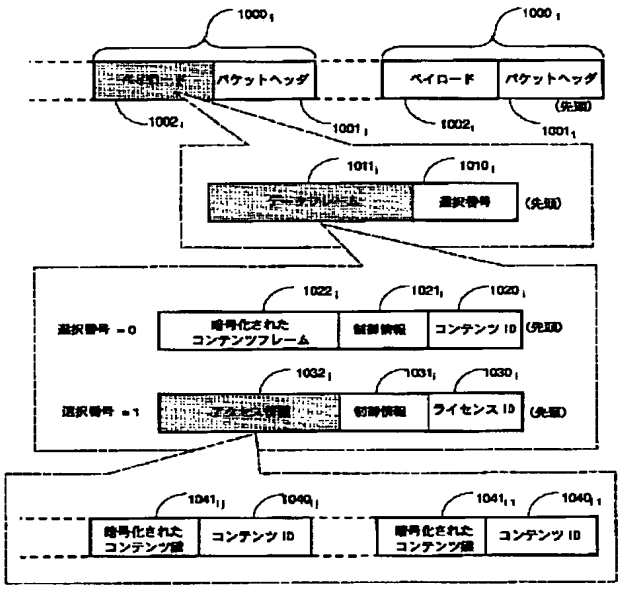
【図４】

図４


ICカードI/F
400
情報処理部
401
情報保持部
402
プログラム保持部
403
ICカード
106
コンテンツ送受信I/F
410
ICカードI/F
411
情報処理部
412
情報保持部
413
コンテンツ蓄積部
414
プログラム保持部
415
表示部
416
ユーザー入力部
417
コンテンツ表示装置
107
108
放送受信部
420
ネットワークI/F
421
コンテンツ転送I/F
422
ICカードI/F
423
情報処理部
424
情報保持部
425
コンテンツ蓄積部
426
プログラム保持部
427
表示部
428
ユーザー入力部
429
コンテンツ蓄積装置

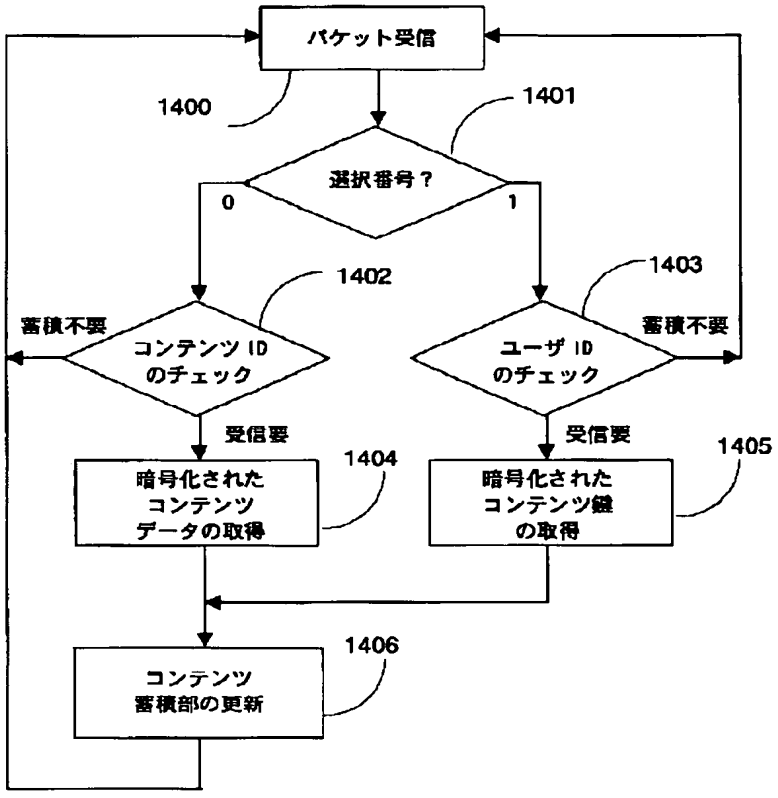
【図１０】

図１０



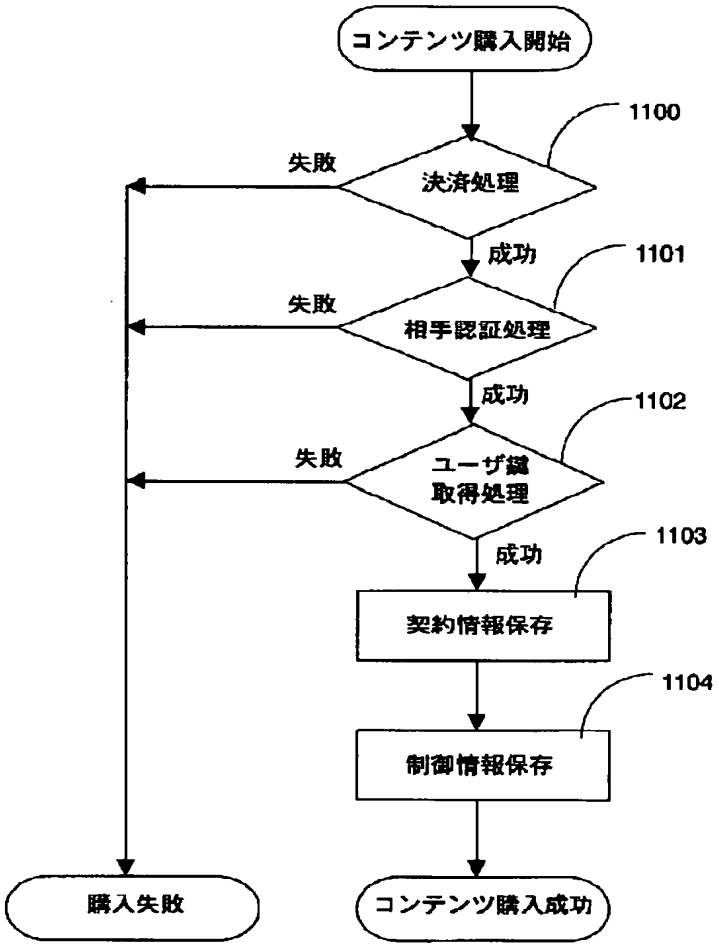
【図１４】

図１４



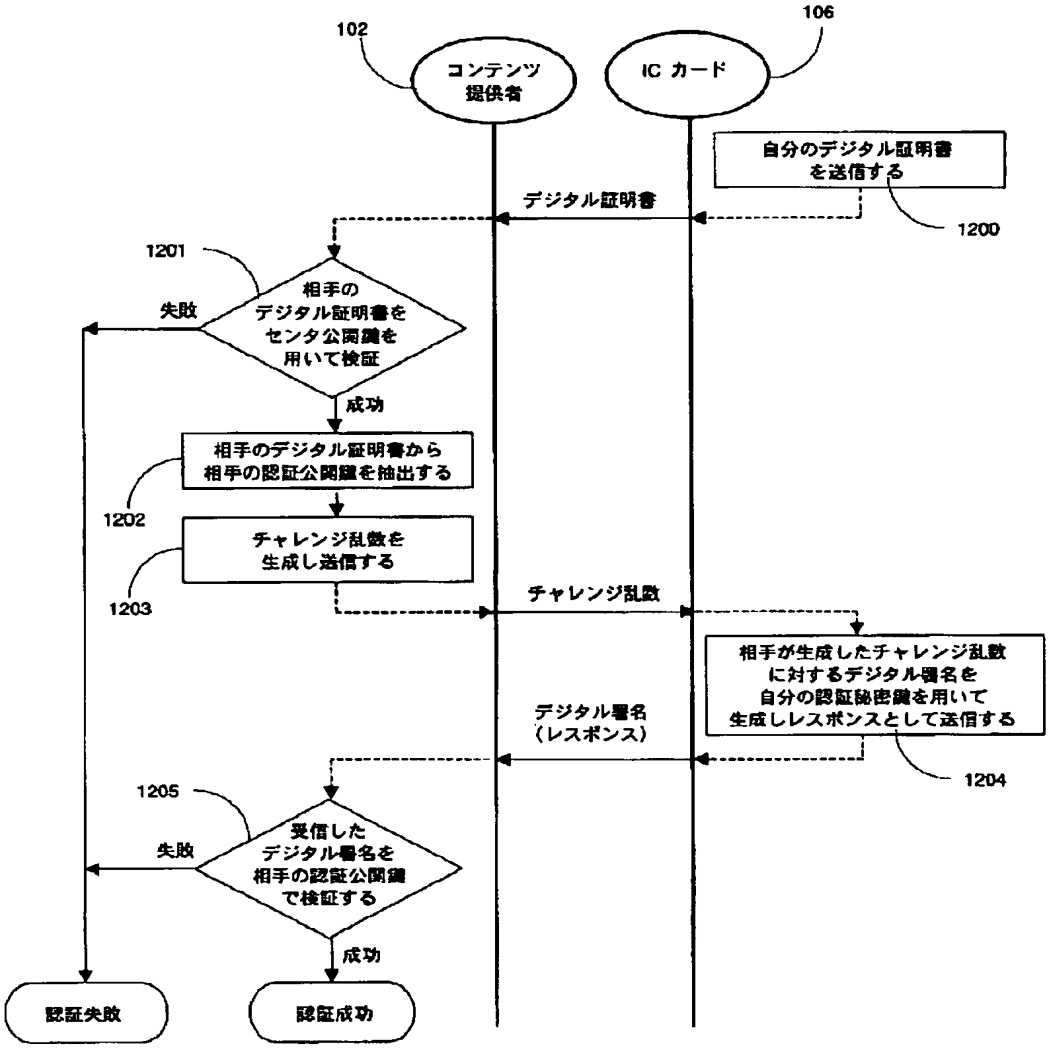
【図１１】

図１１


コンテンツ購入開始
1100
決済処理
失敗
成功
1101
相手認証処理
失敗
成功
1102
ユーザ鍵
取得処理
失敗
成功
1103
契約情報保存
1104
制御情報保存
購入失敗
コンテンツ購入成功

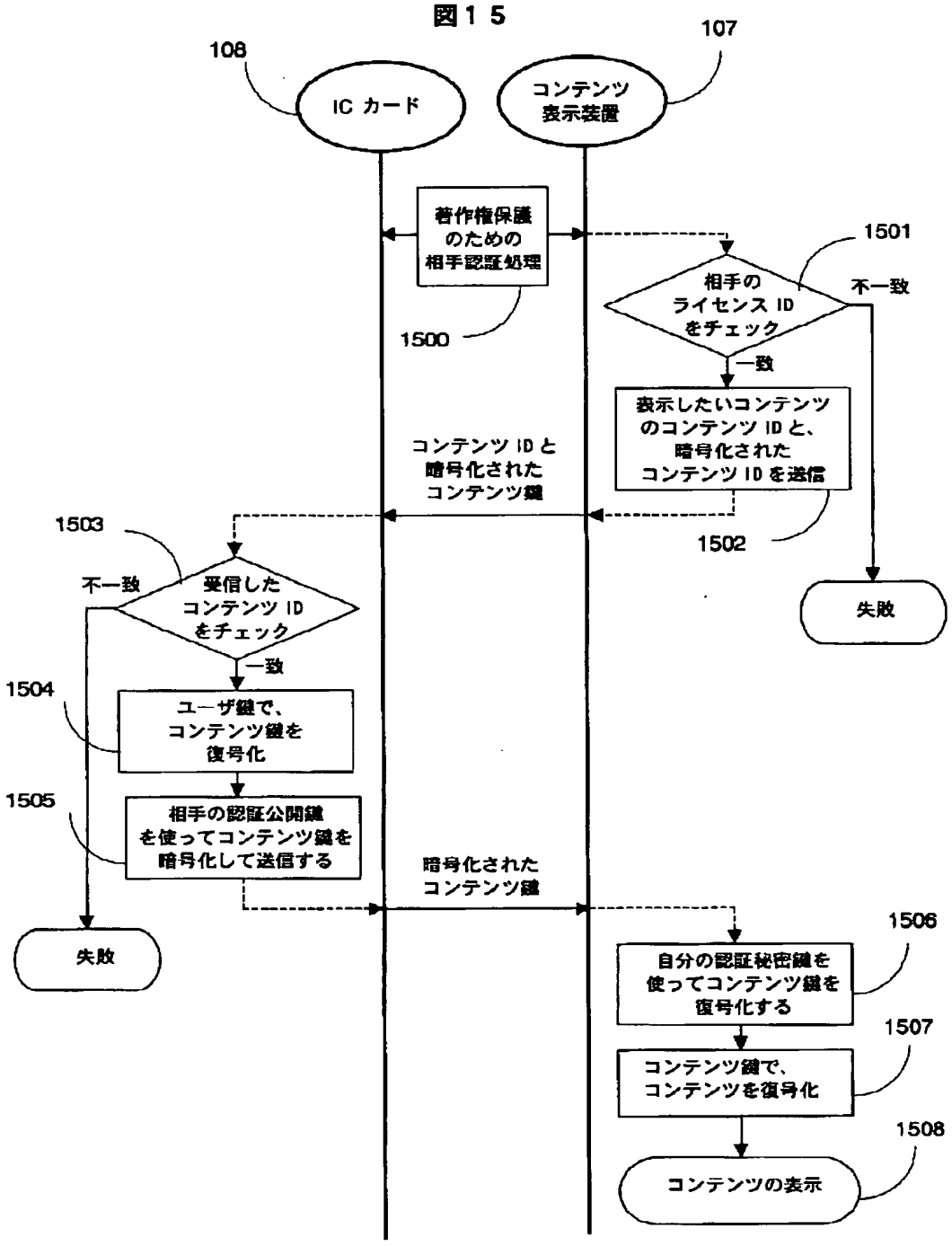
【図１２】

図１２


102
コンテンツ提供者
106
IC カード
自分のデジタル証明書を送信する
1200
デジタル証明書
1201
相手のデジタル証明書をセンタ公開鍵を用いて検証
失敗
成功
相手のデジタル証明書から相手の認証公開鍵を抽出する
1202
チャレンジ乱数を生成し送信する
1203
チャレンジ乱数
相手が生成したチャレンジ乱数に対するデジタル署名を自分の認証秘密鍵を用いて生成しレスポンスとして送信する
1204
デジタル署名（レスポンス）
1205
受信したデジタル署名を相手の認証公開鍵で検証する
失敗
成功
認証失敗
認証成功

【図１５】

図１５



フロントページの続き

(51) Int. Cl.[7]	識別記号	FI		テーマコード（参考）
H04N 7/173	640	H04L 9/00	675A	
		H04N 7/167	Z	

Ｆターム(参考) 5B049 AA05 BB26 CC05 CC08 CC36
DD04 EE01 EE28 FF03 FF04
FF08 GG04 GG07 GG10
5C064 BA01 BB02 BC17 BC18 BC22
BC23 BD02 BD08 CA14 CB08
CC01 CC04
5J104 AA01 AA07 AA12 BA03 EA18
EA22 KA01 KA04 NA03 NA35
PA05 PA07 PA14